Lecture 15: The Agrawal-Kayal-Saxena Deterministic Primality Testing Algorithm (continued)

Algorithmic Number Theory (Fall 2014)
Rutgers University
Swastik Kopparty
Scribe: Prachi Pendse

1 Overview

The last lecture introduced a deterministic primality testing algorithm by Agrawal, Kayal, and Saxena and showed that it ran in time polynomial in $\log(n)$, where n is the number being tested. This lecture will prove the correctness of the algorithm. It is easy to see that if a number n is prime, the algorithm always outputs PRIME as all identities that AKS checks hold.

In order to prove correctness in the other direction, we will suppose n is composite and that the algorithm outputs PRIME. This means that all identities must have held. We will prove relationships between these identities in the next section. In the last section we show that these relationships lead to a contradiction, proving the correctness of the algorithm.

2 Setup

2.1 The AKS Algorithm

1. On input n, if n is a perfect power, output COMPOSITE.
2. Set $R = \log^5(n)$ and $A = \log^6(n)$.
3. If n has any factors $\in (1, R)$, output COMPOSITE.
4. For each $r \in [R]$
   For each $a \in [A]$
   Check that $(X + a)^n \equiv (X^n + a) \pmod{n, X^r - 1}$ by repeated squaring
5. If all identities hold, output PRIME, else COMPOSITE.

From last time, we know $\exists r \leq R$ such that $\mathsf{ord}_r(n) \geq log^2(n)$ and that this r is relatively prime to n. Now suppose n is composite and let p be a prime dividing n such that $r \nmid (p-1)$. Since the algorithm outputs PRIME we know $(X + a)^n \equiv (X^n + a) \pmod{p, X^r - 1}, \forall a \in [A]$.

Definition 1. *Let*

$S = \{Z + a \in \mathbb{F}_p[Z] : a \in [A]\}$

$T = \{n, p\}$

$\mu_r = \{\alpha \in \overline{\mathbb{F}_p}$ *such that* $\alpha^r = 1\}$*, the* r^{th} *roots of unity in* $\overline{\mathbb{F}_p}$.

We now come to the most important definition of this analysis.

Definition 2 (Commuting)**.** *For a polynomial $Q(Z) \in \mathbb{F}_p[Z]$ and an integer $m \in \mathbb{Z}$, we say that Q and m* **commute** *if:*

$$\forall \alpha \in \mu_r, Q(\alpha)^m = Q(\alpha^m).$$

Lemma 3. *If Q_1 commutes with m and Q_2 commutes with m, then $Q_1 \cdot Q_2$ commutes with m.*

Proof. We are given that for all $\alpha \in \mu_r$, $Q_1(\alpha)^m = Q_1(\alpha^m)$ and $Q_2(\alpha)^m = Q_2(\alpha^m)$.

Thus, for all $\alpha \in \mu_r$,

$$Q_1 \cdot Q_2(\alpha^m) = Q_1(\alpha^m) \cdot Q_2(\alpha^m) = Q_1(\alpha)^m \cdot Q_2(\alpha)^m = (Q_1 \cdot Q_2(\alpha))^m.$$

Thus $Q_1 \cdot Q_2$ commutes with m. □

Lemma 4. *If Q commutes with m and Q commutes with m' then Q commutes with $m \cdot m'$.*

Proof. We are given that for all $\alpha \in \mu_r$, $Q(\alpha)^m = Q(\alpha^m)$ and for all $\alpha \in \mu_r$, $Q(\alpha)^{m'} = Q(\alpha^{m'})$.

We have the following simple observation: if $\alpha \in \mu_r$, then $\alpha^m \in \mu_r$.

Thus for every $\alpha \in \mu_r$, we get:

$$Q(\alpha^{m \cdot m'}) = Q((\alpha^m)^{m'}) = Q(\alpha^m)^{m'} = Q(\alpha)^{m \cdot m'}.$$

Hence Q commutes with $m \cdot m'$. □

Definition 5. *Let*

$\overline{S}$ = *the multiplicative closure of S.*

$\overline{T}$ = *the multiplicative closure of T.*

$G = \overline{T} \pmod r = \{n^i \cdot p^j \in \mathbb{Z}_r^*\} \subseteq \mathbb{Z}_r^*$.

$t = |G|$.

By Lemmas 2 and 3, each $Q \in \overline{S}$ and each $m \in \overline{T}$ commute.

Observe that because n and p are relatively prime to r, G is a subgroup of Z_r^*. Since $\mathsf{ord}_r(n) \geq \log^2(n)$, $t \geq \log^2(n)$.

3 Proof of Correctness of AKS Algorithm

3.1 Strategy

1. Fix $\alpha_0 \in \mu_r \subseteq \overline{\mathbb{F}_p}$.
2. Find $\widetilde{m} \neq 0$, $\widetilde{m}$ small, such that $\forall Q(Z) \in \overline{S}$, $Q(\alpha_0)^{\widetilde{m}} = 1$.
3. Find many $Q(Z) \in \overline{S}$ such that $Q(\alpha_0)$ are all distinct.
4. This gives a contradiction: it gives too many roots for the equation $Y^{\widetilde{m}} = 1$.

3.2 Finding many distinct $\widetilde{m}$th roots of unity

We now implement this strategy. Fix $\alpha_0 \in \mu_r$ to be a primitive rth root of 1.

Lemma 6. *There exists an integer $\widetilde{m} \leq n^{2(\sqrt{t}+1)}$, $\widetilde{m} \neq 0$, such that $\forall Q(Z) \in \overline{S}$, $Q(\alpha_0)^{\widetilde{m}} = 1$.*

Proof. It suffices to find nonzero m, $m' \in \overline{T}$ with m, m' small and $m \gneq m'$ such that $\forall Q(Z) \in \overline{S}$, $Q(\alpha_0)^m = Q(\alpha_0)^{m'}$. Setting $\widetilde{m} = m - m'$ satisfies the conditions of the lemma.

Look at $n^i p^j \pmod r : i, j \leq (\sqrt{t}+1)$. Since n is composite, $\exists n^i p^j = m$ and $n^{i'} p^{j'} = m'$, $m, m' \leq n^{2(\sqrt{t}+1)}$ such that $m \equiv m' \pmod r$ and $m \neq m'$. Assume without loss of generality that $m > m'$.

$\forall \alpha \in \mu_r$, $\forall Q(Z) \in \overline{S}$ it holds that

$$Q(\alpha)^m = Q(\alpha^m) = Q(\alpha^{m'}) = Q(\alpha)^{m'}.$$

Thus $Q(\alpha_0)^m = Q(\alpha_0)^{m'} \forall \alpha \in \mu_r$ and $\forall Q(Z) \in \overline{S}$.

Since Q is a product of linear polynomials, α_0 is a primitive r^{th} root of unity, and $r \nmid (p-1)$, we also see that $Q(\alpha_0) \neq 0$.

Because $Q(\alpha_0)^m = Q(\alpha_0)^{m'}$ and $Q(\alpha_0) \neq 0$, we can divide through to get $Q(\alpha_0)^{m-m'} = 1$. Taking $\widetilde{m} = m - m'$ proves the lemma.

□

Lemma 7. *Let $Q(Z)$ and $Q'(Z)$ be distinct polynomials in $\overline{S}$ of degree less than t. Then $Q(\alpha_0) \neq Q'(\alpha_0)$.*

Proof. Suppose $Q(\alpha_0) = Q'(\alpha_0)$ for distinct polynomials $Q, Q' \in \overline{S}$ of degree less than t.

Then $\forall m \in \overline{T}$,

$$Q(\alpha_0^m) = Q(\alpha_0)^m = Q'(\alpha_0)^m = Q'(\alpha_0^m).$$

So Q and Q' agree on every α_0^m for $m \in \overline{T}$. Counting the number of these α_0^m gives

$$|\{\alpha_0^m : m \in \overline{T}\}| = |\overline{T} \pmod r| = |G| = t.$$

But Q and Q' had degrees less than t, so they cannot agree on the t different points α_0^m. Thus it is not possible that $Q(\alpha_0) = Q'(\alpha_0)$ for any distinct polynomials $Q, Q' \in \overline{S}$ of degree less than t, proving the lemma.

□

3.3 Deriving a Contradiction

Observe that $|\{\text{the set of polynomials in } \overline{S} \text{ of degree } < t\}| \geq \binom{A+t-1}{t-1}$.

We also note that $\widetilde{m} \leq n^{2(\sqrt{t}+1)} < n^{3\sqrt{t}} = 2^{3\sqrt{t}\log(n)}$ and $\log^2(n) \leq t$.

Lemma 7 states that the $\binom{A+t-1}{t-1}$ distinct polynomials $Q(Z) \in \overline{S}$ all have distinct values for $Q(\alpha_0)$. By Lemma 6, all these distinct values are $\widetilde{m}$'th roots of unity.

Thus there are $\binom{A+t-1}{t-1}$ distinct $\widetilde{m}^{th}$ roots of unity.

Because $A = \log^6(n) \gg \log^5(n) = R \geq r \geq t$, we can safely assume that $A > 8t$.

Thus $\binom{A+t-1}{t-1} \geq \left(\frac{A}{t}\right)^t > 8^t \geq 2^{3\sqrt{t}\log(n)} \geq \widetilde{m}$.

Since $\binom{A+t-1}{t-1} > \widetilde{m}$, there can not be so many distinct $\widetilde{m}^{th}$ roots of unity, a contradiction.

This completes the proof of the correctness of the AKS deterministic primality testing algorithm.